The Platform Transformation

How IoT Will Change IT, and When

Matthew J. Perry

The Platform Transformation

by Matthew J. Perry

Printed in the United States of America.

Published by O'Reilly Media, Inc., 1005 Gravenstein Highway North, Sebastopol, CA 95472.

O'Reilly books may be purchased for educational, business, or sales promotional use. Online editions are also available for most titles (*http://safaribooksonline.com*). For more information, contact our corporate/institutional sales department: 800-998-9938 or *corporate@oreilly.com*.

Editors: Brian Jepson and Jeff Bleiel

Production Editor: Shiny Kalapurakkel

Copyeditor: Octal Publishing, Inc.

Interior Designer: David Futato

Cover Designer: Karen Montgomery

- August 2016: First Edition

Revision History for the First Edition

- 2016-08-17: First Release

978-1-491-96571-9

[LSI]

The Platform Transformation: How the IoT Will Change IT, and When

Introduction

The Internet of Things (IoT) might be our future, but that future, with its many unknowns, can be a complex place to imagine. Consumers, private enterprise, and governments will all need to make many decisions about how and when to join in the stream of connectivity that is uniting more people, places, and (in the greatest numbers) things every day.

In fact, we have been living in this future for most of a generation. IoT has existed, under different names, since the concept of machine-to-machine (M2M) connectivity was put into practice 20 to 25 years ago. That said, digitization, new connectivity standards, low costs, and the proliferation of IP addresses are taking business to the edge of a new level of complexity.

A distinct *IoT platform* is a relatively new manifestation of the technological trend, but already it is embedded in the landscape. Dozens of companies are offering the services, software, and hardware necessary to take companies into IoT functionality. The marketing is just gearing up, but the field is already robust. According to an IoT Analytics forecast, the IoT platform market is expanding rapidly, and projected to hit $1.6 billion by 2021.

The *IoT stack* is now a distinct creation of hardware, network, and software that brings the power and data of the Internet into working environments in ways that are distinct from the enterprise

IT stack created in the early 2000s. Software platforms that are emerging as the basis for IoT solutions (the aforementioned IoT platforms) can encompass various aspects of the stack, and enable different levels of functionality. Although the number of these platforms is growing, we are beginning to see capability patterns emerge, and thus understand how they best work within business environments and industry verticals to solve problems or create new opportunities.

In its most comprehensive form, the IoT platform will make it possible for a business to connect the disparate parts (things, remote locations, people, etc.), manage those connections efficiently and safely, and harness generated data in the service of business cases.

This report explores key considerations for future proofing elements of the IT stack and smoothing the transition to IoT components for those who will use them.

It's Early: Does It Make Sense to Buy an IoT Platform Now?

Telecom providers have been chasing the potential of IoT long enough to deliver viable products to the market. Leaders in the field have developed robust platforms that they can fairly label "IoT" products as a result of the heightened connectivity, increased data connection capacity, and sophisticated software that they employ. As time goes on, more and more companies will have a clearly identifiable IoT platform at the heart of its technology stack. Platform as a Service (PaaS) has been sufficiently refined, as a concept and a practical delivery for cloud-based services, to provide many choices in the public and private sectors.

The trick for many companies will be to determine which provider and platform can align with their specific business needs and specifications. With an abundance of IoT platforms already in the market—and many more expected—businesses will need to be discriminating and not inclined to view all platforms as equal and interchangeable. They will need to weigh the quality of the components, the scalability across ecosystems of "things," and their suitability to business needs.

That having been said, dynamic solutions are possible for a wide array of

industries and business opportunities. Despite the rapidly changing landscape, IoT platform evolution is already critical to continued competitiveness. The party has begun, and in this case, it's best not to arrive late.

Meanwhile, business models are being turned upside down—and in some cases rendered obsolete—by the implications of connectivity. What IoT represents is not so much physical devices and embedded software that can begin talking to the enterprise, but the connections that link everything together (including customers). It also will redefine usage: who uses the products, data and things, how often they use them, and how often they pay for the privilege. This has implications both for businesses and workers who employ IoT solutions to build and sustain their operations.

Faced with such a potent combination of promise and precaution, enterprises of all sizes, in all industry verticals, need to construct a real-time plan that will clarify several dimensions of the impact of the IoT. That plan should include the following considerations:

- How IoT connectivity can best benefit the enterprise and how adoption can be most efficient in terms of cost and use.
- What impediments to adoption are likely and what existing IT components can be used for IoT solutions as they are phased in.
- Whether IoT upgrades will address ongoing concerns over security and access points.
- How to justify the cost of upgrades, and maintain flexibility and control in contracts with service providers.

This is by no means an exhaustive list of the questions the

technological advances will raise. But it can help to simplify the transition to a world that will be characterized by billions of devices, ever-greater magnitudes of data and expanding area networks.

The technological migration can be most successful when the method, benefits and challenges are clearly delineated. IT upgrades to enable IoT solutions will produce many new challenges to technology leaders, but these should be neither *unforeseen* nor are they insurmountable with today's technologies.

Does the IoT platform require a "rip-and-replace" approach to the legacy IT architecture? Not necessarily. Many companies and industries will find it advantageous to adapt elements of their IT stack when their IoT platform strategy needs to be assessed to support the business requirements that are evolving and growing. Some that focus on applications to deliver services or information might use in-house developers to produce more interactive apps and the means to connect end users. Analytic tools and protocols also can be adopted in stages.

Cost, security, and value projections will influence which parts of an IT platform "migrate" to the IoT first. Contracts with service providers, platform builders, data analysts, and software developers also might affect the pace of development.

IoT Platforms Will Vary in Scope and Function

IoT platforms are distinguished from their predecessors in the IT stack by a proliferation of connectivity between the "things" (which are usually, but not exclusively wireless), edge connectivity, network and cloud services; app enablement technology, analytics and machine learning, and various interfaces (e.g., desktop, mobile).

Over the next few years, we can expect standardization of the

physical and cloud components of the platform, or at least a concentration in the markets as some models and services prove to be better fits to the companies that buy them.

But how can companies choose the best platform and suite of services today? Existing vendor and partner relationships might determine what kind of platform is built. Other companies might need to review recent growth and market potential before determining what type of platform should undergird their business expansion.

Whatever the conditions, there are questions that you need to ask about different layers of the existing IT stack and how they can be affected by an IoT initiative. This report explores the potential of the IoT as it pertains to the following:

- The things and people that are connected to a central control locus.
- The transport method, including network upgrades and new standards of connectivity, especially cloud connectivity.
- Data: where it is stored, where it is needed, and how latency can be minimized.
- Application Programming Interface (API): the backend of applications and the vital containment package and functionality that engages customers but also (and often of more critical value) different layers of the enterprise technology. Whether the end user is a customer or a colleague, smart APIs support the rapidly expanding universe of applications that generate most of the IoT's "wow factor."

- Applications, which like APIs, can face the public or people and things within the enterprise's private network.
- Analytics.
- Interfaces.

Variables

New IoT platforms, both hardware- and software-based, will continue to filter into the tech marketplace for years to come. The differences between hardware platforms and their components, particularly their boards, are worth investigating and comparing. For the purposes of this report, we will focus on the software and middleware components of the IoT platform, because of their variety and the ability of businesses to create their own components, at least on the application and API layer.

Each company will have a distinct experience as it employs IoT components. Some will move faster than others or begin by modernizing one element of the existing IT stack before many of its competitors. Cost of adoption will influence many initial steps because businesses will need to quantify real value and revenue potential in IoT upgrades. In-house developers might build out applications that plug in to an IoT platform, and even create some layers of the platform itself. Here, too, the value propositions must be reviewed in terms of cost savings, ease of use, and reliability.

The influence of open source software will also affect the IoT choices at hand. Open sourcing makes it possible for smaller companies to create solutions to current problems. Although this might introduce yet more protocols to an already complex IoT universe, internal innovation might well be part of the picture. Businesses need to weigh the value of DIY-solutions in terms of time, efficiency, and cost.

There will be a tremendous number of variables and data to consider. But, competent analysis and effective outcomes are possible by keeping primary goals in mind. The IoT will alter standards of connectivity and engagement with end users in and out of the company, but these are means to an end. Decision makers must determine which goals to serve as their operations become more flexible and responsive.

Connecting the Edge—Building-Out the Network

At its most basic, the IoT means many more sensors generating much more data and transmitting it over a wider variety of networks and protocols. These sensors and connected things account for much of the eye-popping IoT growth projections, and their enhanced connectivity—with each other, the cloud, data storage units, and central headquarters—encapsulates the IoT "big idea."

Sensors are only as valuable as the connectivity protocols that service them. In theory, building out a sensor network is one of the less complicated elements of IoT. The development of small, low-power sensors is a driving force behind an industry-grade IoT as well as personal devices. Microelectrical-mechanical systems (MEMS), radio-frequency identification (RFID), and other technologies are important expansions of the IT platform. A sensor network that delivers on its promise—in terms of new data, real-time observation, and cost—will depend on the networks and protocols that connect the edge to the center and the cloud. An important test of IoT quality will be in the gateways, controller software, and security controls that connect to the existing tech platform.

The "edge" exists in a variety of forms, and adopting an IoT platform might not change its boundaries. IoT components can run on the same wide area network (WAN) that a business has been using for years if its assets are grouped together and in proximity with the control center (factories and building HVAC systems are good examples). In these cases, you can implement "short haul" protocols (via Zigbee, LAN cables, Bluetooth, or a variety of other technologies) to knit together the sensor network. Further "long-haul" protocols can provide a major transport lane to the cloud and/or a controller's console.

Depending on the reach and sophistication of legacy IT architecture, this layer of the platform might well be the most abstract, with the fewest immediate impacts on the enterprise. The connective tissue between things and employees who use or monitor data, like most networks we are accustomed to using, will remain the province of service providers or internal IT. For the rest of the enterprise, the sensor layer of the platform will be experienced in the form of results.

The important, preadoption questions surrounding connectivity come back to the data:

What data will be coming up through the platform?

> A retail company tracking merchandise via RFID tags will have different connectivity requirements from that of a municipality with a new network of surveillance cameras. Companies will need to evaluate which connectivity technologies will send required data up the platform through networks that are scalable and sufficiently robust.

Is the data needed in real time?

> Different connectivity methods will function with more or less latency, depending on the content of the data (audio, video, code, etc.). If the data is being analyzed at the time of transmission, the IoT platform will need the capability to extract rich data in an efficient manner.

Is the network bidirectional?

> Shipping companies tracking containers, energy companies relaying instructions to field workers, and banks relaying financial updates will need to utilize protocols that enable the back-and-forth communication, whether it is device-to-device, control center–to-edge, or any other configuration. As protocols

are changing and proliferating quickly, each enterprise will need to analyze its needs carefully before an upgrade.

As the IoT moves into the enterprise, employees will sense the workplace as a fluid organism that reacts as well as thinks. Thanks to refined interfaces that "spell out" more with fewer commands and prompts, the improvements to efficiency will make many jobs easier as a new, real-time "normal" is established. Things, people, and the spaces they inhabit will undergo a mash-up of their own.

Controlling the Data Currents

Data in the IoT age is both the essential element and an inundating force that delivers more than any company can bargain for. The information that industry will generate has the same potential—and the same inundating power—as a body of water. Much as dry climates will need to engineer methods for capturing run-off precipitation, it is imperative that enterprises of all sizes create protocols for keeping critical data from being buried and extraneous streams from increasing latency throughout networks.

IoT data management systems are still in their infancy, and there will be a great deal of refinement of existing management tools, few of which are capable of handling the tremendous new quantities of data.

To begin with, it is helpful to visualize data management as a buffer between the world of sensors and devices and the applications that will make use of the raw material that world of things (and people) generates. The challenge for this layer of the IoT stack deals with both volume and a continuous cycle: not only will there be more data, but it will be arriving at all times. The selection, transmitting and storage processes will need a wide array of tools and a new lifecycle paradigm to maintain continuous function.

A company will need time to determine which streams of data are essential fuel for algorithms and predictive analysis, and which can remain at the level of collection. There is also a need to consider content (video, audio, etc.). Enterprises that can leave a great deal of data on the edge of their networks might need to employ fog computing, or other methods that provide distributed data storage, which can take pressure off central storage and analysis centers.

To create a distributed data architecture, enterprises can adopt a number of technologies to keep communication clear and efficient: WiFi, cellular, RFID, or hybrid technologies might become the standard for keeping the data flow under control and routed to established collection points.

With more data available, more people in an enterprise will be eager to make use of it. This introduces new layers of complexity to the IoT platform's performance. There will be a surge in data requests that will occur at all times throughout the ecosystem. But like the data itself, not all queries are of equal value and priority. IT departments will need to ensure that the appropriate platform capabilities are employed to help aggregate and prioritize both queries and data streams. A key principle to data management is *heterogeneity*: increased variety (and importance) of data, data queries and needs, and the networks that keep them flowing.

Meet the Chief Data Officer

Companies can create a strong framework for IoT expansion by considering a few logistical questions in advance:

- How much data will be generated?
- Where will it travel?

- Will it be bidirectional?
- How much will be needed in real time?
- What protocols will produce the data with minimal latency?

The staggering increases in data and its compounding value will necessitate changes in enterprise structure. Part of every company will be tasked with the ongoing process of coordinating data traffic and stripping away the most valuable assets. The “chief data officer” (CDO) might soon be a standard in the C-suite. A data management team may well be necessary to work across the organization and ensure that all sectors are receiving the data and insights they need as well as streamlining collection and collaboration.

The IoT is often twinned with the objective of breaking down siloes: separate departments in an enterprise that do not collaborate with other departments and take a proprietary approach to the collection and securitization of their data. This is a case for which the IoT’s impact extends beyond underlying technology and effects change in corporate structure.

A data management department, led by a CDO with a strong team, can set ground rules for how data is shared, prioritized, and secured throughout the enterprise and value chains. Even in smaller companies, the basic principle of data’s ubiquity will take root: all players will need to consider what accumulated data means for future decisions and for the company at large. Data, as the fuel for the IoT engine, needs to end up in the right places to extract its value.

Data Lakes and Warehouses: Do You Need Both?

Repositories for data are nothing new, but in traditional IT models, the data "warehouse" usually had an entrance and no exit. Furthermore, tools and protocols for sifting through the data and refining it were limited.

The data warehouse is a familiar concept at this point because enterprises have been storing and categorizing information for a generation. But as the volume of information expands as more connected things generate ever-more data, companies might feel the need to find new homes for the excess.

By most definitions, warehouses store data that has been processed, picked over and categorized for its usefulness. The warehouse collects and collates information with assigned value, rather than raw material. IT platforms have well-established security and access protocols for warehouses because there has been ample time to define and protect them.

In contrast, *data lakes* are repositories for data that has not been structured or evaluated. A lack of established protocols means that it is often easier to "swim" through a lake than "walk" through a warehouse, but it also means that lake security is still a work in progress.

The IT platform migrating to the IoT might find use for a data lake as more data from more sensors and connected things is generated. We can conduct a great deal of real-time analysis in the data lake, which can exist on the edge of an enterprise and away from the cloud. For instance, feeds from a surveillance camera network that "comes online" might be directed first to a data lake, and much of it might remain there. Other feeds, such as those from sensors that enable predictive maintenance, might move to the data warehouse after first being collected in the data lake.

Enterprises considering an IoT platform will need to determine if spikes in data generation will require new repositories. There are cost implications for analytics, as well: will data be so valuable that it is worth hiring analysts to qualify and quantify it?

Engineering the Data Management System

Data management is about automation: working at all times to identify data packets and send them to their appropriate destinations. The IoT technology will be designed to make these judgment calls automatically. But it will be up to company strategists to decide on a management strategy. To that end, a few basic questions should be considered:

How much data can remain on the edge?

Not all data needs to be analyzed and repurposed. The performance specifications of the data management system should be outlined clearly before this part of the IoT solution is put in place. Questions about the amount of bandwidth needed, peak usage times, the content of data (video, audio, and images), the time-sensitivity of data, and the flow of transmission (one way or bidirectional) will all affect the decisions and choices about IoT components. If a company depends on low latency (minimized disruptions due to heavy traffic) to send directions quickly, configurations will need to account for this requirement.

Edge computing and data storage can be a boon to enterprises with many employees or smart devices working outside the control center. An energy company with many meters to read, or a department store with many security cameras, can realize operational cost savings by keeping feeds needed only on the edge from traveling to the cloud.

How and where should you mash up data?

The IoT promises to raise the level of analytic complexity and improve actionable results by allowing disparate datasets to mingle and create a multidimensional picture. But where should this integration occur? Companies must decide if a central data warehouse can become sufficiently multifunctional, or whether a complex data network will need to be created to enable mash-ups on the enterprise edge.

The IoT promises to raise the level of analytic complexity and improve actionable results by allowing disparate datasets to mingle and create a multidimensional picture. But where should this integration occur? Companies must decide if a central data warehouse can become sufficiently

multifunctional, or whether a complex data network will need to be created to enable mash-ups on the enterprise edge.

The trick will be to take data aggregation to the next step and treat the data as a service as well as a commodity. Data virtualization software and tools are becoming a more cost-effective way to promote the necessary integration of data coming through disparate channels. Data virtualization can act like a translation device that can tie databases, warehouses, cloud components and operation systems into a single, comprehensible format. They will play an increasingly important role in the data delivery systems of many companies.

"Stream analysis" is another catchword that spells out the need to make immediate use of captured data. Platform as a Service (PaaS) offerings are increasingly focused on pushing Big Data into the cloud and enacting the give-and-take principle of the IoT and greater speed.

How do you analyze dark data?

Data generation is critical, but it means little if the systems to pull its value are not in place. Open software options like Hadoop have become extremely popular, and they will continue to play an important role in the quest for more data convergence and increased benefit from analysis of the data.

But we will need additional methods to extract more from the Big Data scoops that the IoT platforms will provide. Streaming data analytics and other capabilities will attempt to dive into the massive reserves of *dark data*. Companies have been compiling dark data for years in the form of emails, personal storage tables, ZIP files and other fallout from business operations. As the IoT becomes the standard, dark data—and untapped value—inevitably will multiply.

The vast majority of what we call “Big Data” is dark: unused, out of sight, with stores of untapped value—or potential problems. Reliable estimates classify 90 percent of big data as the dark variety.[1]

An IoT platform can generate value by integrating with dark data reserves via Hadoop or other Big Data software and channeling it into streams of data on the surface.

The analysis of that data will present a greater challenge. Dives into dark data can be cost prohibitive because they depend on the skill and initiative of data analysts, a workforce segment still in short supply.[2] It can be tempting for companies to utilize existing analysts for this task, but there are potential problems because the search for value in data requires not only technical expertise, but also a sense of how to discern value for the enterprise or its customers.

How can you use a digital twin?

Along with 3D printing, digital facsimiles of machines are beginning to suggest huge changes to predictive analytics and real-time maintenance. Sensors and data feeds attached to a machine can help create a structure that looks, operates, and responds to stimuli in the exact same way as its “real” twin. It’s a concept that is set to explode with the IoT, with potentially much lower cost and far higher functionality than digital models in recent years.[3]

A digital twin is a function of things (the devices and products generating data), connectivity (working to bring networks together), data management (cloud computing, storage, and analytics), and applications. As such, they likely will figure heavily into the construction and logic of IoT platforms.

The implications of digital twins are extensive and potentially

mind-boggling, but they have immediate relevance to the IoT platform, and their adoption might well be a component of many adoption strategies. At one time an exclusive part of design, digital twins can keep "learning" thanks to new data sources and the expansion of predictive analytics in IoT platforms. Importantly, however, many aspects of digital-twin creation are possible through creative use of apps and software.

The digital twin can look more like a data mash-up than an actual facsimile of the physical twin. There is a need to link the product requirements and use cases with the digitized read-out of the physical functions. You must first have in place the right connectivity, 3D digital model, and applications that know how to use that combination for the twins' "binding" to deliver benefits.

Data outside a comparative framework loses much of its value. The digital twin will be, for many companies, the means by which standards for function, response, and maintenance are established.

End-Users, APIs, and Applications: Keeping Connections In Line with Business Value

The lower layers of the IoT platform are all critical, but now we reach the presentation layer. Here is where most employees will interface with and feel the urgency of the new technology. They also will encounter some headache-inducing challenges.

For most enterprises, the IoT will mean many more data feeds as sensors, tags, and networks proliferate. Even with an "out-of-the-box" IoT platform, there will be many operations to adapt and change: routing protocols, data retrieval paths, authentication processes, and the like. But just as important will be the top-layer decisions about what to do with the data and who uses it. The nontechnical protocols will influence the technical ones, and vice

versa.

APIs are where existing IT and the IoT come together most directly, and where the shift can be very confusing and time consuming.

No matter how APIs are provided, the platform supporting them must enhance two critical features: *scalability* and *speed*. Data and connected things from the edge are primed for explosive growth. For the increase to be managed within acceptable parameters of adjustment and reconfiguration, the platform provider must supply products that can parallel a company's growth.

As the effects of the IoT are felt more widely, exploiting changes in a marketplace or user preferences (internally or externally), applications will need a powerful, flexible platform supporting them. For employees, the key difference will be learning how to adapt to and anticipate changes that the turbocharged IoT platform can enable.

The IoT API

The IoT guarantees the creation of many more apps and services. IoT versions of the API will multiply on a parallel track as end users search for more complex interfaces, and app development times become shorter. There also will be the need for apps to patch into more layers of the platform to exploit data. APIs that facilitate backend access (and cut down on the need for coding expertise) might well be the crux of the new intersection of business and IT in the enterprise.

Public APIs are critical to establishing the connections to a company's customers and app users. The best API will bring the valuable data into contact with those who need it, with low latency and intuitive interfaces. A company might employ a distinct IoT platform for its API if it needs to tie together different

groups of customers or facilitate transactions.

In essence, the function of APIs will remain the same. The changes IoT will enable are based on scope, complexity, and interactivity. Unlike other aspects of the IoT platform, there will not be out-of-the-box APIs and networks. Updates will have to patch in with legacy systems and software; it will take time for the necessary coding to be executed, and much of it might be more difficult than what was needed to patch into earlier API generations. The API extends into the stack to connect with other systems, but for the most part it enables the application layer of the stack. It will take time for the full potential to be realized, and it might require expanding the IT department to bring in the talent necessary to grapple with the more challenging engineering.

But as the API becomes a more dynamic playing field, companies will need to ensure that it's not just IT that steps up its game. An API is a conduit for core business values to reach targeted audiences (customers, disparate parts of the business, partners, etc.). But as it becomes an IoT component, the API also will be interacting with the cloud, and in many cases with devices and things. If the API is the hub of a wheel, in its IoT iteration the hub will be connected to many more spokes.

That means the teams servicing and providing the API might expand or change as a company's IoT platform becomes more complex. Currently, many companies provide their own APIs. In the future, many more might partner with another company that provides the API platform. Even if the work is accomplished in-house, the team will expand. To determine the sources and depths of values, the IoT API will need more developers (working the backend) and marketing experts onboard. This can effect changes on job descriptions and team organization as more elements of the business move into the cloud.

Although these developments will take time, it is important to

think in advance about how the IoT will change the API equation. Here are a few particular questions to ask:

What happens to the old API connections and protocols?

> For purposes of security and operability, companies will need a plan for decoupling apps and other elements in the network linked to the legacy API. This might necessitate changes in service contracts and added device management options.

How does the IoT change network priorities?

> More data and more connections mean more links to the API. Will the design need to reflect preference for emergency operations, customer interfaces, or machine shutdowns? Company strategists will need to affirm that the IoT version of the API is engineered to back up essential operations.

Is asset management and security robust?

> Apps will still be crucial on an IoT platform, and over time their numbers are certain to increase. More apps mean more developers, quality control, data analysts, and so on. They all will need access to the API, but for how long should they have it? How are other API functions and gateways protected against unsupervised or prohibited access?

The Apps: Where Experimentation and Peak IoT Experience Intersect

Like many other aspects of the IT platform, legacy app development—despite innumerable successes—is overmatched when it encounters the IoT and its potential. App development time is decreasing, but to take advantage of accelerated market opportunities and customer preferences, the process must speed up even more.

The IoT does present a few solutions at the outset. Software-based apps generally are easier to build in the cloud, using protocols that do not require as much specialized programming knowledge. Therefore, the backlog of requests from the enterprise can be whittled down if IT focuses more on building out apps and services that require less development skill and time commitment. As development tools become easier to use, it might be possible for tech-savvy workers (and good strategists) to take on “last mile” developments and relieve IT of some of its burden.

There will be a fine line between taking initiative on refining an app interface and actually building the app. But as IoT protocols become more available, companies will need to think through the best use of human resources and possibly revise development protocols.

Some analysis argues that the Internet has broken down the boundaries between IT and the rest of the enterprise. When everyone interacts with the Internet to do business, no one can afford to stay in the dark regarding the role of digital capabilities. Even if employees are not sufficiently skilled to make minor adjustments to apps, they need to learn to recognize the signs that apps are underperforming. There will be plenty of such signs—particularly among mobile apps—as market currents shift and upgrades enable some functions and render others outmoded. Simultaneously, IT will need to apply use-case lenses to their work.

As building tools become more intuitive and easier to use, businesses might see a burst of innovation from departments that traditionally waited for marketing or IT to make their contributions before adapting their interface with customers or other end users. Assuming that a company uses a developed IoT platform for support, it can put its programming muscle into creating the mash-ups and apps that provide a distinctive view and presentation to customers and users.

The IoT difference at the application layer will be characterized by complexity taken to scale. The smart city is perhaps the quintessential example. Although any municipality is a collection of "companies" (i.e., services), the interdisciplinary use of data is key to the vision of a modern landscape. As the IoT proliferates, disparate systems will share information and blend it together for a more comprehensive approach to functionality and quality of life. Public-private partnerships can foster the development of app systems that become more sophisticated and multifaceted over time.

It is easy to extrapolate similar changes spreading through private companies taking advantage of interoperability that blends functions and operations through a series of connected apps and services. As coding requirements become less demanding and app development moves even more to the cloud, the teams around app development will change, and the roles of each team member will change as the app environment is enriched and linked to parallel environments.

Facing this much change (with so much embedded potential), the rules of governance in IT departments might begin to seem unnecessarily restrictive. Here is another tricky balance to maintain as IoT functionality increases demand for more apps and more products in less time. Enterprises cannot afford to be hidebound by outdated quality and security control, but extreme relaxation of standards can open the door to the potential disasters that keep IT decision makers awake at night.

Security: Everything and Everywhere, for Everyone

A fully securitized IoT platform might seem like an impossible dream. Billions of connected devices will carry billions of IP addresses. Millions of gateways might be accessible to millions of workers. If a company with 5,000 employees provides each one

access, in some form, to this endlessly interconnected platform, how many opportunities for a breach will occur each day?

To do business in the digital age is to be exposed to the risk of digital crime. As stated by Verizon, “No locale, industry, or organization is bulletproof when it comes to the compromise of data.”[4] Security regularly rates as the primary concern of maintaining networks, and many companies are ready to switch vendors if they feel current security solutions are insufficiently robust.

In response, the online security industry has shifted into overdrive. Cybersecurity is a mammoth industry with a projected value of $170 billion in 2020.[5] With so many resources and the alarms already ringing, why are companies still so concerned about security?

It might be true that security concerns did not keep pace with growth in the first phase of the Internet expansion, and there is no guarantee that all players in the cybersecurity market will provide top-notch systems that do not create more problems than they solve. But IoT platforms are being designed with security as an intrinsic priority. Although nothing is foolproof, enterprises (both public and private) of all sizes have ample reason to be confident about the improving quality of security systems.

Nonetheless, human beings are still in (or out of) control; error and malfeasance in the last mile of security controls will be tough to eradicate. Thanks to our imperfections, IoT security is no more immune to threat than padlocks and keys. As business ecosystems become more complex, and partnerships evolve, the threat of contagion will remain. There will be circumstances in which companies with insufficient protection at gateways are rendered as vulnerable as their least secure partner. With the variety of protocols available to devices, security can become complicated quickly.

Yet, the threats are not all enabled by gross human error. Hackers have, and will, exploit imperfections in security software. IoT platforms will rely more on automated security, and yet much of the firmware associated with mobile and web-based devices operates from disparate standards. For every imperfect fit, there is the potential for a breach. Even a company with the most scrupulous practices for security could, in theory, fall prey to a brilliant hack of an automated security system. Because IoT connectivity predates a full suite of software patches and prescriptive tools, even the best IoT platform vendors are playing catch-up, and will be for some time.

Secure Partnerships are Key to a Secure IoT

The growing popularity of IoT platforms demonstrates the fact that many companies realize an in-house solution is too costly, too time consuming or too intricate. This applies just as much to IoT security features as any other level of the platform.

So, the migration into IoT capabilities often begins with a wise partnership. Platform providers should not only have a robust product with solid, ingrained security protocols. They also should be willing to discuss the security challenges they have already faced, and be realistic about their current methods of shipping patches throughout the ecosystem. Ultimately, each company will be looking for a security provider that acknowledges the risks and is proactive about correction.

As companies move into the IoT, they might be looking to connect a wide variety of things that carry different licensing and security features. Making sure they all conform to the ingrained security features of a platform will take time and diligence. Companies will think twice about bringing more edge devices online if the means to secure them is insufficient or too time consuming. However, many security features developed in legacy IT environments can

cross over to the IoT: public and private key cryptology, segmentation, and shutdown protocols can be adapted to handle network expansion.

What Will the Company Do to Stay Safe?

Cloud capabilities are essential to many aspects of IoT expansion. The sense of the cloud as a naturally insecure environment is pervasive, but in fact, security experts have been working to make cloud applications and servers just as safe as private networks. But as an incremental approach, companies can ask if *every* network of things needs to be cloud-connected. Companies with service branches or localized sets of assets (such as a factory) might not need the cloud to effectively manage them. If the IT platform-to-IoT platform process is gradual, some parts of the network can remain local or cloud optional. With a single gateway to send necessary data to an aggregation layer, some corners of the enterprise can remain security stable while others move into an IoT paradigm. Conversely, companies can create test beds out of remote or underutilized sites to assess security challenges before going enterprise wide (the same principle can apply to updating and configuring cloud-based apps). Like all other cyber security features, this approach has its limits.

Security Standards for Employees

As more companies embrace a bring your own device (BYOD) approach, there will need to be corresponding changes to policies that cover loss, theft, downloads, passwords, and other potential security impacts.

Certification and compliance standards will need review, and regular audits of the security system will need to be deployed.

Many companies have responded to the accelerated digitized

marketplace by reevaluating performance review, the conceptual question being, “if it now makes sense to review corporate objectives on a quarterly basis, why should employees still be evaluated annually?” This thinking can be applied as well to security audits, and probably should be when the platform is moving into IoT capability.

Other established practices will need to be reevaluated and extended, including inventories, identification of sensitive data, backup and access protocols, and encryption policies. In most of these cases, the objective is to review existing methodologies and update them based on the corresponding extension of the network. Writing a completely new rule book, in most cases, will not be necessary.

Employees might need to undergo more training to drive home the heightened need for security. Performance reviews might well yield metrics that indicate how much security has become part of the culture. Workers’ observance of passwords, encryption protocols, and device management will need to be emphasized to an even greater degree than existed in the traditional company structure. Regular training events that introduce new security rules and concerns should keep pace with the company’s extension into the IoT universe.

Conclusion: A Journey Outward, in Stages

The enterprise approach to connecting devices, sensors, and machines has been in progress for almost 20 years. The proliferation of proven technologies and the growth of the Internet are creating a new set of capabilities for all “things.” In the process, the M2M universe, from which IoT sprang, denotes a far more restricted and separated reality than what we see today. Through the introduction of new applications, interfaces, and the “knowledge” they generate about the things we use, our expectations for a technology’s platforms performance have been

transformed.

The upside of this migration is that the next steps in this process will not seem entirely foreign. Sound business practices and use cases will still be the name of the game for any company. Rather than employing IoT devices, networks, and security to stay apace of competition, the smart objective is to use the technology to solve an existing problem or fulfill an outstanding aspiration for better service, better maintenance, or more data-rich decision making.

That said, the acceleration provided by an IoT platform can be sharp, forceful, and uncomfortable. Companies must prepare for the surge in new data, predictive models, and real time functionality. Security protocols must be reviewed with platform improvements in mind so that newly opened doors do not invite cyber malfeasance.

Dialogue with new or existing service providers will need to be detailed, informed, and inclined toward the business objectives of the company. The IoT will change the vendor landscape as much as it changes users; existing service contracts and security protocols will need to be reviewed to ensure that they can adapt to keep companies flexible as IoT capabilities expand.

Perhaps most important, the enterprise needs to dissolve any silo that once provided IT with exclusive housing. Every decision-maker will need to consider the technological implications of each use case that utilizes the IoT platform. IT experts will need to keep the larger picture in mind: IoT connectivity for its own sake might be redundant, insecure, or not worth the cost in money or time. Employees of all types will need to keep abreast of security requirements. They must also think about their roles in terms of reaching customers and partners in new ways.

The IoT-empowered company will be a work in progress for some

years to come. But with sufficient preparation and analysis, there is no need to delay the future.

---

1 See IDC, FutureScape: Worldwide IT Industry 2016 Predictions—Leading Digital Transformation to Scale. IDC dark data estimate predates this study.

2 Davenport, T. H. and Patil D. J. 2012 Data Scientist: The Sexiest Job of the 21st Century. *Harvard Business Review*.

3 See PTC Confidential: The Digital Twin: Bridging the Physical & Digital Worlds. October 2015, and *www.thingevent.com*.

4 Verizon 2016 Data Breach Investigations Report.

5 Cybersecurity Market Reaches $75 billion in 2015; Expected to Reach $170 billion by 2020. *Forbes Tech*, December 2015.

About the Author

Matthew J. Perry is a writer and editor with a particular interest in how the Internet of Things can make cities smarter. He has written for Cisco Systems and collaborates regularly with experts in tech, finance, and marketing. A collaborator on 10 published books, he lives in New York City with his family.